

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2001-242785

(P2001-242785A)

(43) 公開日 平成13年9月7日 (2001.9.7)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード* (参考)
G 0 9 C 1/00	6 4 0	G 0 9 C 1/00	6 4 0 B
			6 4 0 Z
	6 6 0		6 6 0 A
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 2 0 B
			3 2 0 F

審査請求 未請求 請求項の数 3 O L 公開請求 (全 8 頁)

(21) 出願番号 特願2001-123147(P2001-123147)

(22) 出願日 平成13年4月20日 (2001.4.20)

(71) 出願人 000102728

株式会社エヌ・ティ・ティ・データ
東京都江東区豊洲三丁目3番3号

(71) 出願人 501161756

社団法人東京銀行協会
東京都千代田区丸ノ内一丁目3番1号

(71) 出願人 399035766

エヌ・ティ・ティ・コミュニケーションズ
株式会社
東京都千代田区内幸町一丁目1番6号

(74) 代理人 100064908

弁理士 志賀 正武 (外2名)

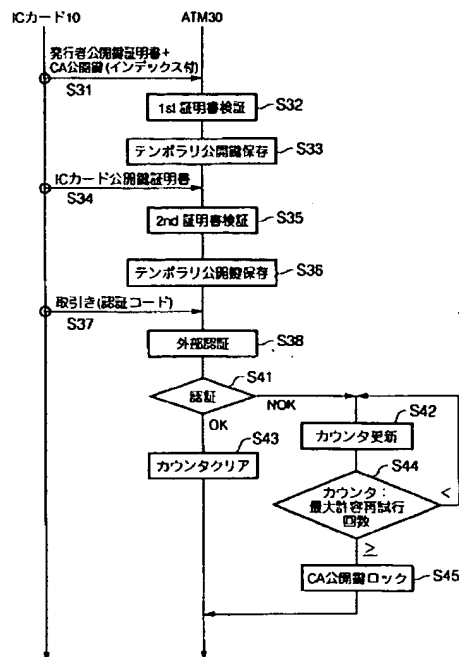
最終頁に続く

(54) 【発明の名称】 デジタル署名システム

(57) 【要約】

【課題】 秘密鍵を複数持つデジタル署名システムにおける公開鍵の特定と、複数階層の証明書検証処理の効率化をはかる。

【解決手段】 どの秘密鍵を利用した証明書を特定するためのインデックスを付与してノードに送信し、当該ノードでインデックスに関連付けられた公開鍵を特定して検証を行なう。また、あるノードで証明書が検証された公開鍵をICカード10の一時記憶領域に格納し、この公開鍵を指定して次のノードにおける証明書の検証を行ない、更に検証された公開鍵を用いて外部認証コードを検証し取引を行なう。



【特許請求の範囲】

【請求項1】 秘密鍵を複数持つデジタル署名システムにおいて、
どの秘密鍵を利用した証明書かを特定するためのインデックスを付与してノードに送信し、当該ノードで前記インデックスに関連付けられた公開鍵を特定して検証を行なうことを特徴とするデジタル署名システム。

【請求項2】 少なくとも2つのノードで証明書を持ち、前記各証明書を検証した後、当該検証された公開鍵を用いて外部認証コードを検証しカード取引を行なうデジタル署名システムにおいて、

前記あるノードにおいて前記証明書が検証された公開鍵をICカードの一時記憶領域に格納し、前記一時記憶領域に格納された公開鍵を指定して次のノードにおける証明書の検証を行ない、前記検証された公開鍵を用いて外部認証コードを検証し、カード取引を行なうことを特徴とするデジタル署名システム。

【請求項3】 前記外部認証コードの検証に失敗した場合、最初に利用した公開鍵に付加されたカウンタに設定される最大許容再試行回数を超えたときに前記公開鍵の利用を禁止することを特徴とする請求項2に記載のデジタル署名システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、複数世代の公開鍵管理と複数階層の証明書検証を実現するデジタル署名システムに関する。

【0002】

【従来の技術】デジタル署名は、公開鍵暗号化方式や秘密鍵暗号化方式と組み合わせて複合的なシステムの中で利用される。公開鍵暗号化方式を利用することから、実用するためには認証局(CA)が運営される。

【0003】デジタル署名を金融機関に適用した場合の認証局体系および証明書管理について図6にその概要が示されている。図6において、符号61は金融機関、符号62は認証局、符号63はATM等の金融端末、符号64はICカードである。まず、認証局62(以下、単にCA62と称する)は、金融機関61の申請に基づき証明書の発行を行うスキーム管理局である。カード発行者である金融機関61は、CA62に自身の公開鍵を登録し、当該鍵に対する証明書を発行してもらう。また、金融機関61は、自らが発行する各ICカード64に対する公開鍵、秘密鍵のペアを作成し、自身の秘密鍵によって証明書を生成する。ATM等金融端末63においては、個々の端末に対する公開鍵、秘密鍵のペアを作成し、CA62により生成された証明書をATM等金融端末63に格納する。

【0004】ところで、上記した公開鍵暗号化方式では、安全性の根拠の一つを、解読の際における計算量の多さにおいている。従って、同一の公開鍵や秘密鍵を長

期間使用し続けることは安全性の低下につながるため、証明書の発行者は、それに付与するデジタル署名の生成用秘密鍵を定期的に更新しなければならない。その際、現在のサービスを中断することなく、かつICカード64とATM等金融端末63との間の認証に必要なデータの整合性を確保した管理に基づく必要がある。

【0005】

【発明が解決しようとする課題】これに対し、従来のICカード64におけるATM等金融端末63を利用した証明書検証によれば、ある領域に格納された公開鍵を用いて検証が行なわれるため、CA62の秘密鍵の更新に同期して更新される公開鍵を入手する必要があり、上記した定期的な更新により2種類以上の証明書が出回る可能性があつて、ICカード64ではその整合性を加味した検証を行なうことはできなかった。

【0006】また、従来、ICカード64内に保持する公開鍵を用いて証明書を検証するのに、その証明書を検証するコマンドとは別に、検証され、取り出された公開鍵を用いて外部認証コードの検証を行なうコマンドの実行を要していた。従って、金融システムのように、証明書の検証が、CA62-外部ノード発行者(金融機関61)-外部ノード(ICカード64)といった複数階層を持つものにおいては、それぞれの階層における証明書の検証で得られる公開鍵が次の階層における証明書の検証に反映されず、従って、繰り返しの動作により、効率的な証明書の検証、公開鍵の抽出ができなかった。特に、検証に失敗した場合等においては、証明書のデータ量が比較的大きいため、少ない記憶容量しか持たないICカードにあっては致命的な問題となる。

【0007】本発明は上記事情に鑑みてなされたものであり、ICカードにCA公開鍵とその世代を示すインデックスとを組み合わせて複数格納し、ICカードで外部ノードの公開鍵証明書を検証する場合、公開鍵証明書と共にその証明書を付与したCAのインデックスと共にICカードに送信し、ICカード内で格納されたデータと送信されたデータを照合し関連付けられたCA公開鍵を用いて検証することにより、セキュリティを高め、かつ、信頼性及び処理速度の向上を図ったデジタル署名システムを提供することを目的とする。

【0008】また、ICカードの公開鍵証明書を検証するコマンドに、一時的に格納された鍵を用いて検証するインタフェースを付加することにより、CA公開鍵を用いた証明書が検証された公開鍵を一時記憶領域に格納し、その公開鍵を指定して次階層の証明書の検証を行ない、外部認証を行なうことができ、複数階層の証明書検証を効率的に、かつ、記憶容量の節約と汎用性の向上を図ったデジタル署名システムを提供することも目的とする。

【0009】

【課題を解決するための手段】上記した課題を解決する

ために本発明は、秘密鍵が複数存在するデジタル署名システムにおいて、どの秘密鍵を利用した証明書かを特定するためのインデックスを付与してノードに送信し、当該ノードで前記インデックスに関連付けられた公開鍵を特定して検証を行なうことを特徴とする。

【0010】上記した課題を解決するために本発明は、少なくとも2つのノードで証明書を持ち、前記各証明書を検証した後、当該検証された公開鍵を用いて外部認証コードを検証しカード取引を行なうデジタル署名システムにおいて、前記あるノードにおいて前記証明書が検証された公開鍵をICカードの一時記憶領域に格納し、前記一時記憶領域に格納された公開鍵を指定して次のノードにおける証明書の検証を行ない、前記検証された公開鍵を用いて外部認証コードを検証しカード取引を行なうことを特徴とする。

【0011】また、本発明のデジタル署名システムにおいて、前記外部認証コードの検証に失敗した場合、最初に利用した公開鍵に付加されたカウンタに設定される最大許容再試行回数を越えたときに前記公開鍵の利用を禁止することを特徴とする。

【0012】上記構成において、ICカード内にCA公開鍵とそのCAのインデックスを組み合わせて複数格納し、ICカードで外部ノードの公開鍵証明書を検証するとき、公開鍵証明書と共にその証明書を付与したCAのインデックスと共にICカード内に送信し、ICカードでは、その格納されたCAのインデックスと送信されるCAのインデックスとを照合し、関連付けられたCA公開鍵で検証することで、複数種類の秘密鍵による証明書が出回ってもICカードでの検証を可能とし、セキュリティを維持しながら信頼性及び処理速度の向上が図られる。また、上記構成において、CA公開鍵を用いて証明書が検証された公開鍵はテンポラリ公開鍵としてICカード内に保存され、ICカードの証明書を検証するコマンドを用いてそのテンポラリ公開鍵を指定し、当該テンポラリ公開鍵を用いて証明書を検証し、証明書が検証された公開鍵はテンポラリ公開鍵として保存される。そして、外部認証時、そのテンポラリ公開鍵を用いた検証を行なうことで、ICカードの記憶容量の節約ができ、また、1つのコマンドで証明書の検証ならびに公開鍵の抽出を実現できるため、検証のための処理速度の改善がはかれる。

【0013】

【発明の実施の形態】図1は、本発明が採用されるICカードの内部構成を示すブロック図である。ICカード10は、CPU11を制御中枢とし、プログラムメモリ12、データメモリ13、入出力インタフェース回路14が内部バス15に共通接続されて成る。入出力インタフェース回路14は、ATM端末等外部から到来するコマンドもしくはデータを受信して内部バス15を介してCPU11に伝える他、CPU11によって処理された

データを外部に供給する双方向の回路である。

【0014】CPU11は、プログラムメモリ12に記録されたプログラムに従いデータメモリ13を使用して内部処理を行なう。データメモリ13には、アプリケーション毎、EF (Elementary File) が割り付けられ、DF (Directory File) で示されるアプリケーションを格納する領域に対し、例えば、キャッシュカード取引、デビットカード取引を行なうための複数種の取引データが格納される。本発明と関係するところでは、どの秘密鍵を利用した証明書かを特定するためのインデックスと関連付けられた公開鍵が格納される領域Aの他に、CA公開鍵を用いて証明書が検証された公開鍵を保存するためのテンポラリ領域Bが割り付けられている。

【0015】図2は、本発明に従う鍵管理の一例を表形式で示した図である。図2において、各発行者の公開鍵および秘密鍵に付与されている番号がその対応関係を示している。図中、証<秘1>とは、CA秘密鍵1を用いて生成された公開鍵証明書を表し、“公1”とは公開鍵1を表す。なお、図2では、秘密鍵の有効期間によってフェーズを区分しており、CAでの鍵管理、金融機関（発行者）での鍵管理、ICカード10へ格納する発行者証明書および鍵、ATM端末30へ格納する端末公開鍵証明書および鍵のそれぞれの鍵更新スケジュールが示されている。ICカード10および端末の欄に記載されている矢印は、その期間において、証明書および公開鍵を新規に作成、または更新する場合にはどのような内容になるかを示す。例えば、サービス開始時において、新規のカードを発行する場合には、証明書<秘1or2>、ならびに公開鍵1および公開鍵2を設定することになる。

【0016】ところで、ICカード10とATM端末30において保持している証明書、公開鍵が異なる場合がある。その場合は、上記したように、証明書作成に用いた秘密鍵と対応する公開鍵が公開鍵インデックとして指定されているため、その指定された公開鍵を用いて認証処理を行なう。すなわち、ICカード10内には、CA公開鍵とそのCAのインデックスとを組み合わせて複数格納されている。そして、ICカード10内で外部ノードの公開鍵証明書を検証する場合、その外部ノードでは、公開鍵証明書と共にその証明書を付与したCAのインデックスと共にICカード10内に送信する。ICカード10では、内部で格納されたCAのインデックスと送信されたCAのインデックスとを比較照合して、等しいものが見つかったときにそれに関連付けられたCAの公開鍵で検証する。このインデックスにより現在有効となっている公開鍵が特定できる。

【0017】図3に、ICカード10、ATM端末30のそれぞれにおけるCA公開鍵および証明書の格納形態が、それぞれ、(a)、(b)で示され、また、図4に証明書検証処理の動作概念が示されている。図3に示されるように、証明書鍵発行者であるCAの鍵の更新時に

においてその運用やサービスを制限することなく、当該鍵を更新することに対応するため、ICカード10内部には、2組のCA公開鍵とCA公開鍵インデックス（ICカード検証用）、1組の発行者公開鍵証明書、ICカード公開鍵証明書とCA公開鍵インデックス（ICカード・証明書）を持つ。カード10内部への関連データの格納形態は図示したとおりである。ここでは、RSA暗号化の例が示されている。証明書データは、対応するCA公開鍵に付与されているCAインデックス（ICカード・証明書）と関係付けられる。

【0018】外部から証明書データを受信すると種々のチェックを実行後、デジタル署名の検証が行なわれる。この検証は、ICカード10内部における2つのCA公開鍵の組のうち、端末公開鍵証明書とCA公開鍵インデックス（ICカード・検証用）が等しい組のCA公開鍵を利用する。この様子は図4に示されている。どちらのCA公開鍵インデックス（ICカード・検証用）とも異なる場合、および正常に終了しなかった場合はコマンド処理を中断する。

【0019】図5は、カード認証の流れを説明するために引用した図であり、具体的には、図6に示される「CA-発行者（金融機関）-ICカード」から成る階層化された公開鍵管理体系における、証明書検証ならびに公開鍵抽出シーケンスが示されている。ここでは、上記した公開鍵管理体系の中で、ICカード10とATM端末30間の動作シーケンスのみ抽出して示している。

【0020】動作説明に先立ち、カード発行者である金融機関は、CAに自身の公開鍵を登録し、当該鍵に対する証明書を発行してもらう。また、金融機関は、自らが発行する各ICカード10に対する公開鍵、秘密鍵のペアを作成し、自身の秘密鍵によって証明書を生成する。更に、ATM端末30においては、個々の端末に対する公開鍵、秘密鍵のペアを作成し、CAにより生成された証明書をATM端末30に格納してあるものとする。

【0021】上記した前提の下、まず、ATM端末30は、ICカード10から発行者公開鍵証明書、CA公開鍵およびその世代番号が示されるインデックス他の情報を読み出す（ステップS31）。これら情報を得たATM端末30は、内部でSET PUBLIC IC KEYコマンドを発行し、第1階層、ここでは発行者公開鍵証明書の検証を行なう（ステップS32）。SET PUBLIC IC KEYコマンドは、外部ノードから送られる公開鍵の証明書をICカード10内に格納されている公開鍵またはテンポラリ公開鍵を用いて検証し、当該公開鍵をATM端末30内に設定するために使用されるコマンドであり、本コマンドで設定した公開鍵は、再度本コマンドを使用して設定するまで、または、設定した公開鍵を用いた認証コマンドが実行されるまで有効とするものである。

【0022】特徴的には、このSET PUBLIC IC KEYコマンドには、ICカード10の証明書を検証するコマ

ンドにCA公開鍵を用いて検証するインタフェースが備えられていることである。ここで得られるCA公開鍵を用いて証明書が検証された公開鍵は「テンポラリ公開鍵」としてICカード10内の一時記憶領域Bに保存される（ステップS33）。直後、SET-PUBLIC-IC-KEYコマンドにより、上記により設定された「テンポラリ公開鍵」を指定してICカード公開鍵証明書の内部にある公開鍵を抽出して第2階層、ここでは、ICカード公開鍵証明書の検証を行ない（ステップS34、S35）、テンポラリ公開鍵を保存する（ステップS36）。

【0023】更に、キャッシュカードやデビットカードによる取引があったとき（ステップS37）、先に設定された公開鍵に基づき、認証コマンド（EXTERNAL AUTHENTICATE）を用いて外部認証（暗号化されたデータ内容のチェック）を行なう（ステップS38）。なお、テンポラリ公開鍵が設定されていて、テンポラリ公開鍵を用いた外部認証に失敗した場合は（ステップS41）、テンポラリ公開鍵を設定する際、最初に利用した鍵（ATM端末30に記録されているCA公開鍵）の再試行回数がカウントアップされ（ステップS42）、成功した場合はクリアされる（ステップS43）。また、再試行回数がATM端末30に設定されている最大許容再試行回数を超えた場合にはCA公開鍵がロックされる（ステップS44、S45）。再試行回数および最大許容再試行回数はCA公開鍵に関連付けられているものとする。

【0024】以上説明のように、CA公開鍵を用いて証明書が検証された公開鍵はテンポラリ公開鍵としてATM端末30内に保存され、ICカード10の証明書を検証するコマンドを用いてそのテンポラリ公開鍵を指定し、当該テンポラリ公開鍵を用いて次階層の証明書を検証し、証明書が検証された公開鍵はテンポラリ公開鍵として保存される。そして、外部認証時、そのテンポラリ公開鍵を用いた検証を行なうことで取引が実行される。このように、テンポラリ公開鍵の利用により複数階層の検証が大量の証明書データの送信なくして可能となる。なお、上記した実施形態では、ATM端末30が階層化された証明書検証および公開鍵抽出を行なうものとして説明したが、ICカード10に置換えても同様に実行可能である。

【0025】

【発明の効果】以上説明のように本発明によれば、ICカード内にCA公開鍵とそのCAのインデックスを組み合わせて複数格納し、ICカードで外部ノードの公開鍵証明書を検証するとき、公開鍵証明書と共にその証明書を付与したCAのインデックスをICカード内に送信し、ICカードでは、その格納されたCAのインデックスと送信されるCAのインデックスとを照合し、関連付けられたCA公開鍵で検証することにより、複数種類の秘密鍵による証明書が出回ってもICカードでの検証を可能とし、セキュリティを維持しつつ信頼性及び処理速

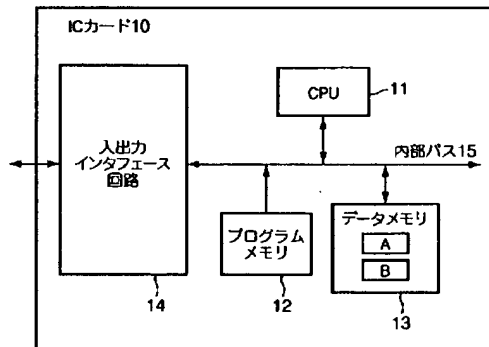
度の向上を図ることができる。

【0026】また、CA公開鍵を用いて証明書が検証された公開鍵はテンポラリ公開鍵としてICカード内に保存され、ICカードの証明書を検証するコマンドを用いてそのテンポラリ公開鍵を指定し、当該テンポラリ公開鍵を用いて次階層の証明書を検証し、証明書が検証された公開鍵はテンポラリ公開鍵として保存される。このことにより、複数階層の証明書の検証を実現でき、外部認証時、そのテンポラリ公開鍵を用いた検証を行なうことで、ICカードの記憶容量の節約ができ、また、汎用的なコマンドを複数回実行することで、証明書の検証ならびに公開鍵の抽出を実現できるため、検証のためのICカードのプログラム容量の削減、拡張性の改善が図られる。

【図面の簡単な説明】

【図1】 本発明において使用されるICカードの内部

【図1】



構成を示すブロック図である。

【図2】 本発明のデジタル署名システムによる鍵管理の一例を表形式で示した図である。

【図3】 ICカード、ATMのそれぞれにおけるCA公開鍵および証明書の格納形態を説明するために引用した図である。

【図4】 本発明実施形態の動作を説明するために引用した図であり、証明書検証処理の動作概念図である。

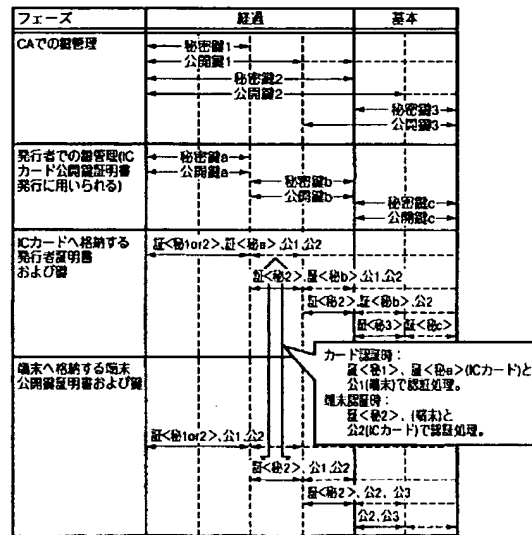
【図5】 本発明のデジタル署名システムの動作をシーケンスチャートで示した図である。

【図6】 本発明の前提となる証明書発行体系を説明するために引用した図である。

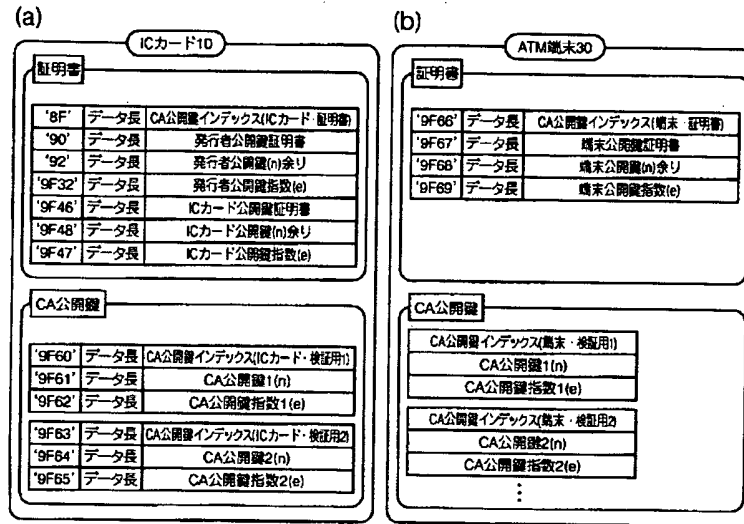
【符号の説明】

10…ICカード、11…CPU、12…プログラムメモリ、13…データメモリ、14…入出力インタフェース回路15…内部バス、30…ATM端末

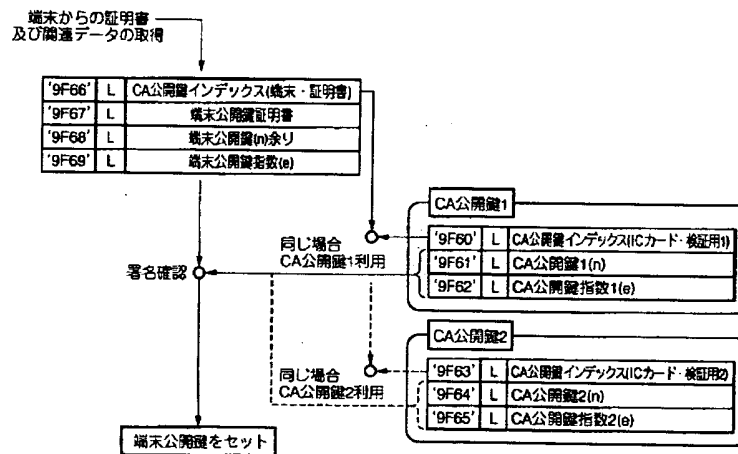
【図2】



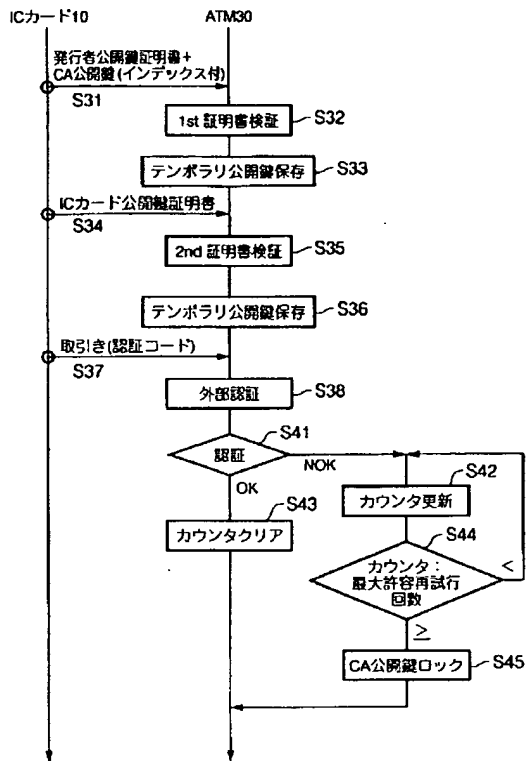
【図3】



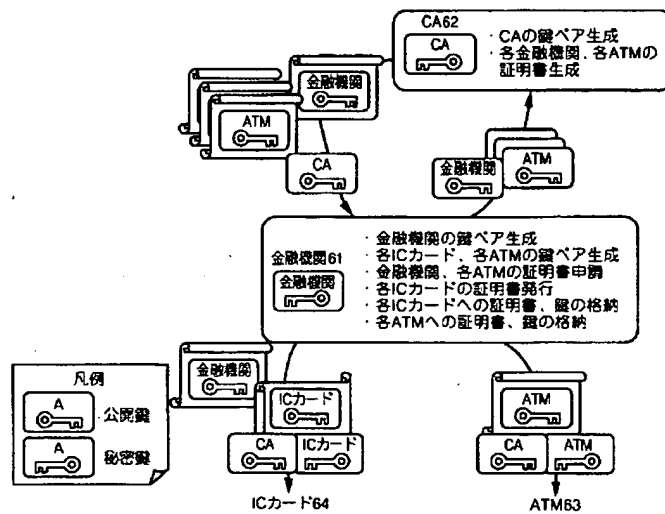
【図4】



【図5】



【図6】



フロントページの続き

(72)発明者 星川 知之
東京都江東区豊洲三丁目3番3号 株式会
社エヌ・ティ・ティ・データ内
(72)発明者 岩瀬 史幸
東京都江東区豊洲三丁目3番3号 株式会
社エヌ・ティ・ティ・データ内
(72)発明者 三輪 哲也
東京都江東区豊洲三丁目3番3号 株式会
社エヌ・ティ・ティ・データ内

(72)発明者 増田 豊
東京都千代田区丸ノ内一丁目3番1号 社
団法人東京銀行協会内
(72)発明者 前田 亮
東京都千代田区内幸町一丁目1番6号 エ
ヌ・ティ・ティ・コミュニケーションズ株
式会社内
(72)発明者 奥平 進
東京都千代田区内幸町一丁目1番6号 エ
ヌ・ティ・ティ・コミュニケーションズ株
式会社内